AFFIDAVIT

I, Gregory L. Newberry, United States Postal Inspector with the United States Postal Inspection Service ("USPIS") Memphis, Tennessee, being duly sworn, state as follows:

1. I have been a Postal Inspector with the USPIS for twelve years. Prior to serving as a Postal Inspector, I was a Special Agent with the U.S. Department of Housing and Urban Development, Office of Inspector General for four years and a Police Officer with the Memphis Police Department for five years. Over the past 21 years, I have led, conducted, and/or participated in criminal investigations of matters and offenses such as mail theft, burglary, robbery, complex financial schemes, narcotics trafficking, mortgage fraud and identity theft.
2. I am currently assigned to investigate criminal offenses involving the United States Postal Service ("USPS"), including Title 18, United States Code, Section 1028A (Aggravated Identity Theft), Title 18, United States Code, Section 1029 (Fraud and Related Activity in Connection with Activity Devices), Title 18, United States Code, Section 1344 (Bank Fraud), and Title 18, United States Code, Section 1708 (Mail Theft).
3. The facts set forth in the instant affidavit are based upon my personal observations, my training and experience, and information that I obtained from other law enforcement officers familiar with the investigation. Because the instant affidavit is being submitted for the sole purpose of establishing probable cause, it does not purport to represent or set forth all of my knowledge of, or investigation into, the instant matter. Rather, I have set forth facts that I believe are sufficient to establish probable cause for the issuance of the requested search warrant. Unless specifically indicated otherwise, all conversations and statements described are related in substance and in part only.

GN

ELECTRONIC DEVICES TO BE SEARCHED

4. This application seeks to obtain a search warrant for evidence of violations of Title 18, United States Code, Section 1028A (Aggravated Identity Theft), Title 18, United States Code, Section 1029 (Fraud and Related Activity in Connection with Activity Devices), Title 18, United States Code, Section 1344 (Bank Fraud), and Title 18, United States Code, Section 1708 (Mail Theft). The electronic devices include a black thumb drive, gold Apple iPhone 13 in pink case, pink HP laptop computer with model number 14-cb172wm and serial number 5CD2024485, and a silver HP laptop computer with model number 15-dw1033dx and serial number CND14534XP. The electronic devices are currently located at USPIS Memphis Domicile, 161 E. GE Patterson Avenue, Memphis, Tennessee 38103, a place within the Western District of Tennessee.

INVESTIGATION

5. On June 7, 2022, USPIS Memphis Field Office received information from Meredith Wooten (hereinafter "Wooten"), General Counsel, with Centerline Business Services about some of their checks being stolen from the U.S. Mail. Inspector Gregory Newberry contacted Wooten in order to gain additional information. Wooten relayed sometime during February 2022 several commercial checks had been stolen after they were deposited in U.S. Postal Service ("USPS") blue collection boxes at White Station Post Office. Wooten stated they also placed some commercial checks in the USPS blue collection box at Bartlett Post Office which were also stolen. Wooten advised the checks were ultimately counterfeited and deposited into bank accounts. Wooten stated Centerline Business Service is an equity management company that had approximately 77 Limited Liability Corporations as clients. Wooten stated all of the stolen commercial checks were against some of their clients' bank accounts. Wooten added that Centerline Business Services

GN

address was 813 Ridge Lake Blvd., Memphis, Tennessee 38120, and their clients' addresses listed on their commercial checks were the same. Wooten advised the current loss was approximately $262,000.00.

6. Wooten relayed that on or about June 7, 2022, she received a call from Trooper James Pruitt (hereinafter "Pruitt") with the South Carolina Department of Public Safety. Wooten stated the call was about a traffic stop he made in Greenville, South Carolina. During the search of a rental vehicle, Pruitt discovered several checks in their clients' names. Wooten stated the checks were against clients Colbert Matz Rosenfelt LLC, LR Nelson Consulting Engineering LLC, Callaway Architecture LLC, Triton Engineering LLC, WGM Design LLP, and AM Engineering LLC. Wooten stated all the counterfeit checks were against bank accounts at Fifth Third Bank. Wooten informed Inspector Newberry that she would forward him the email chain related to her communications with Pruitt. Wooten added that Pruitt also located stolen and counterfeited checks from other cities to include Little Rock, Arkansas; Kansas City, Missouri; Germantown, Tennessee; and Baltimore, Maryland. Wooten stated that Pruitt informed her he had reached out to law enforcement agencies in the aforementioned cities.

7. Inspector Newberry contacted Pruitt regarding the information received from Wooten. Pruitt stated on May 14, 2022, he was on routine patrol on Interstate 85N in Greenville, South Carolina, when he observed a vehicle violate a traffic law. Pruitt advised he conducted a traffic stop and when he approached the driver, he could smell the odor of marijuana emitting from the vehicle. Pruitt stated the driver informed him he was coming from a concert in Atlanta, GA. Pruitt stated he ultimately detained the driver, CARTER BULLOCK (hereinafter "BULLOCK"), and front seat passenger, SHAKYLA SPRAGLEY (hereinafter "SPRAGLEY"). Pruitt added that BULLOCK and

GN

SPARAGLEY were from Richmond, Virginia and were occupying a rental vehicle with a Virginia license plate. Pruitt relayed he searched the vehicle and discovered marijuana, a handgun, several checks in different business names, debit cards in different names, two (2) laptop computers, a cell phone, blank check stock, a printer, thumb drive, and check writing software. Pruitt added that he was not familiar with white collar investigations but suspected BULLOCK and SPRAGLEY were involved in identity theft. Pruitt stated he arrested both BULLOCK and SPARAGLEY and seized the aforementioned items as evidence. Pruitt stated he later contacted law enforcement in Little Rock, Arkansas because one of the seized checks was from a business in Little Rock. Pruitt stated he spoke with Lt. Bryan Brown with Little Rock Police Department and informed him about the matter. Pruitt relayed Lt. Brown informed him he was going to reach out to a postal inspector in Little Rock about the matter. Pruitt stated he reached out to a U.S. Secret Service agent named Andrew Muska in Baltimore, Maryland and a law enforcement officer in Kansas City, Missouri. Inspector Newberry noticed that Lt. Brown and Detective Muska were included in the email chain forwarded by Wooten. Pruitt advised he would email Inspector Newberry copies of his Criminal Enforcement Report, Seizure Warrants, seized checks, seized debit cards, and arrest warrants.

8. Inspector Newberry contacted Postal Inspector Eric Doyle from USPIS Little Rock Domicile to inquire about the matter. Inspector Doyle stated he received information from Lt. Brown about the stolen check from his territory and was handling the case with Detective Clemmons with LRPD. Inspector Doyle stated he was not going to pursue investigation because only one check was recovered during the traffic stop. Inspector Newberry contacted Detective Muska with Baltimore County Police Department and he stated he was a Task Force Officer with U.S. Secret Service. Detective Muska stated he

GN

was handling the joint investigation with Postal Inspector Jesse Arguetta. Inspector Newberry contacted Postal Inspector Kyle Parker from USPIS Grenville Domicile and inquired if he was familiar with the matter. Inspector Parker stated he was familiar with the case after receiving a call from Pruitt. Inspector Parker stated he spoke with Inspector Arguetta in Baltimore and was informed by Inspector Arguetta that he was not pursuing prosecution because there was only one check from his jurisdiction. Inspector Parker stated he was not going to investigate the case because there were not any victims in his jurisdiction. Inspector Newberry requested Inspector Parker to retrieve the evidence from South Carolina Department of Safety and send it to him. Inspector Parker agreed to send all the evidence seized by Pruitt.

9. On June 8, 2022, Wooten called Inspector Newberry and relayed that she discovered two additional checks which had been stolen from USPS collection boxes at Bartlett Post Office. Wooten stated one of the stolen commercial checks was against their client's account named National Network Services LLC. Wooten stated the check was in the amount of $149,406.32 and was successfully negotiated in Fairfax, Virginia. Wooten stated the check was against National Network Services' Regions Bank account. Wooten stated the other stolen check was against their client's account named Ascension Property Services in the amount of $9,023.00. Wooten stated Ascension Property Services' bank account was also with Regions Bank. Wooten added that the Ascension Property Services' check was also successfully negotiated.

10. Inspector Newberry conducted research on BULLOCK and SPRAGLEY using law enforcement databases. Inspector Newberry determined BULLOCK had previous arrests for Shoplifting, Obtaining Money - Fraud False Pretenses, Grand Larceny, and Contempt of Court. SPRAGLEY had a previous arrest for Failure to Appear. On June 24, 2022,

GN

Inspector Newberry received the evidence shipped by Inspector Parker. Inspector Newberry reviewed copies of the counterfeit checks seized from the rental vehicle and discovered some of the checks were made payable to individuals purportedly with Richmond, Virginia addresses including Shacole Jones, Ebony Davis, Jahliesha Smith, and Tajanae Bruce. Inspector Newberry conducted research on Facebook and located BULLOCK's Facebook page. Inspector Newberry discovered BULLOCK was friends on Facebook with Shacole Jones, Ebony Davis, Jahliesha Smith, and Tajanae Bruce.

11. While reviewing the evidence, Inspector Newberry also observed a counterfeit check written against a business named Wolf River HG located in Germantown, Tennessee. The check number was 101974 in the amount of $8,617.68 and was made payable to "Joseph Louis" with an address of 2170 Elkridge Lane, Richmond, Virginia 23223. Inspector Newberry discovered Wolf River HG was located at 3165 Forest Hill Irene Road in Germantown. Inspector Newberry contacted Deana Spangler (hereinafter "Spangler"), Business Manager, with Wolf River Hospitality Group. Spangler relayed they had commercial checks stolen from the mail sometime during March 2022 and April 2022. Spangler stated the checks were deposited into a USPS blue collection box near 5570 Murray Avenue in Memphis, Tennessee. Spangler provided Inspector Newberry with a list of 21 commercial checks which were mailed but never arrived to their intended recipients. Spangler added that she had to stop payments on the 21 checks with Simmons Bank. Spangler relayed that only one counterfeit check had cleared their Simmons Bank account.

CONCLUSION

12. Based on the above-described investigation, the Affiant believes probable cause exists that there will be located on the two (2) laptop computers, cell phone, and thumb drive,

GN

evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1028A (Aggravated Identity Theft), Title 18, United States Code, Section 1029 (Fraud and Related Activity in Connection with Activity Devices), Title 18, United States Code, Section 1344 (Bank Fraud), and Title 18, United States Code, Section 1708 (Mail Theft). Specifically, your Affiant believes, based on his training and experience, laptop computers and cell phones can be used to access bank accounts and credit card accounts. Affiant knows that a laptop computer and cell phone can be used to make fraudulent transactions against unsuspecting victims' bank accounts and credit card accounts if a suspect has an access device such as a bank account number, company name, and bank routing number. Affiant also knows that laptop computers, thumb drives, and printers can be used to create counterfeit checks.

13. Additionally, based on Affiant's knowledge, training, and experience, Affiant believes that persons engaged in identity theft, bank fraud, and access device fraud possess and maintain cell phones and computers, which include the central processing units, external and internal drives, external and internal storage equipment or media, terminals or video display units, and peripheral equipment, such as CD-ROM duplicators, fax machines, copies, keyboards, printers, modems, programmable telephone dialing devices, etc., to communicate with others, maintain records, and to commit the fraud.

14. Based on Affiant's knowledge, training, and experience, Affiant knows that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct respects: (1) the items themselves may be instrumentalities, fruits, and/or evidence of crime; and/or (2) items may have been used to collect and store information about crimes (in the form of electronic data). Thus, Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize

GN

computer hardware, software, documentation, passwords, and data security devices which are: (1) instrumentalities, fruits and/or evidence of crime; and/or (2) storage devices for information about crimes.

15. Based on personal knowledge, training, and experience, the Affiant knows that searching and seizing information from cell phones and computers often requires agents to seize most of all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because computer storage devices can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal evidence; he or she might also store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and often it would be impractical to attempt this kind of search on site.

16. Searching cell phones and computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. For example, on site and laboratory analysis by a qualified computer specialist is often required in order to properly retrieve and analyze electronically stored data, document and authenticate the data, and prevent the loss of the data either from accidental or deliberate programmed destruction. In many cases, the evidentiary data can be backed up to government owned computer data storage devices at the site of the search. However, there are circumstances that may necessitate the seizure and removal of the entire computer system to a secure laboratory setting in order to analyze and extract the evidence.

GN

Gregory L. Newberry
U.S. POSTAL INSPECTOR

Subscribed and sworn to before me on this 29th day of June 2022.

Honorable Charmiane G. Claxton
UNITED STATES MAGISTRATE JUDGE

GN